IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 3, 2020, accepted February 17, 2020, date of publication February 27, 2020, date of current version March 10, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2976798

Image Compression and Encryption Scheme Based on Compressive Sensing and Fourier Transform

MIAO ZHANG[1], XIAO-JUN TONG[1], JIE LIU[1], ZHU WANG[1], JINLONG LIU[1], BAOLONG LIU[1], AND JING MA[2]

[1]School of Computer Science and Technology, Harbin Institute of Technology, Weihai 264209, China
[2]Science and Technology on Information Assurance Laboratory, Beijing 100072, China

Corresponding author: Xiao-Jun Tong (tong_xiaojun@163.com)

This work was supported in part by project ZR2019MF054 supported by Shandong Provincial Natural Science Foundation, in part by the Foundation of Science and Technology on Information Assurance Laboratory under Grant KJ-17-004, in part by the 2017 Weihai University Construction Project, in part by the Equip Pre-research Projects of 2018 supported by the Foundation of China Academy of Space Technology under Grant WT-TXYY/WLZDFHJY003, in part by the National Natural Science Foundation of China under Grant 61902091, in part by Fundamental Research Funds for Central Universities under Grant HIT.NSRIF.2020099, and in part by the Engineering Technology and Research Center of Weihai Information Security.

ABSTRACT An image compression and encryption scheme based on compressive sensing (CS) and Fourier transform is proposed to achieve image encryption and compression with reconstruction robustness and high security. Making use of the property of CS, encryption and compression are combined. In order to avoid the security limitations of revealing the energy information of the plaintext from ciphertext and reusing of measurement matrix to improve security, chaos system and two-dimensional fractional Fourier transform (2D-FRT) are used to perform encryption. Moreover, double random phase encryption based on 2D-FRT can avoid the loss of reconstruction robustness in diffusion encryption. The test results indicate that the proposed method has high security, good compression performance and reconstruction robustness.

INDEX TERMS Image compression and image encryption, compressive sensing, fractional Fourier transform, chaotic map.

I. INTRODUCTION

At present, a series of related theories developed based on compressive sensing (CS) have also been proposed, such as model-based CS theory, structured CS theory, and spectral CS theory. For image compression coding, Orsdemir *et al.* [1] proposed a data compression and reconstruction algorithm based on CS. The measurement matrix used in this algorithm is the non-coherent random projection matrix in each sensor. Gan *et al.* [2] proposed a CS coding method for image block based on CS, which greatly reduced the complexity of compression and reconstruction of large data volume images. Sarkis and Diepold [3] applied CS theory to depth image compression and proposed a depth image compression scheme with better compression performance than JPEG and JPEG2000. Du *et al.* [4] proposed a two-dimensional geometric signal compression method with high compression ratio, high speed, and excellent reconstruction performance based on CS. Yang *et al.* [5] encoded different parts of the image and proposed a random adaptive image CS method with high reconstruction quality. Due to the rapid development of neural-network technology [6], CS framework based on neural-network has also been proposed [7]. At this stage, the application field of CS is expanding, such as compression and encryption for medical 3D images [8] and wireless energy auditing networks [9].

When the random measurement matrix in the CS framework is used as the key, the CS can also be regarded as an encryption scheme. Therefore, compared with the traditional encryption scheme, the CS theory can achieve both compression and encryption. In combination with image encryption, Rachlin [10] analyzed the security of a noise-free CS measurement matrix for strictly sparse signals and verified good compression and encryption effects. Zhang *et al.* [11] believed that the random measurement matrix is the key to the CS encryption scheme. Therefore, a random binary sparse

The associate editor coordinating the review of this manuscript and approving it for publication was Sun Junwei.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see http://creativecommons.org/licenses/by/4.0/

matrix is used to construct the measurement matrix, which can recover the signal with high efficiency. And an image encryption scheme based on CS is designed. Although the algorithm has good security, the computation and size of key are too large to be practical. Zhang *et al.* [12] proposed a new idea of using secret orthogonal basis as the sparse basis for CS, therefore designed a new image compression and encryption method. Most of the CS based image compression schemes mentioned above use the entire measurement matrix as a key, they make the consumption and storage space of key too large. Moreover, this kind of CS based encryption scheme cannot resist chosen-plaintext attack.

In recent years, due to the superior performance of chaos in image encryption, chaos theory [13], [14] and chaos-based image encryption methods [15], [16] have developed greatly. Therefore, some encryption schemes combining CS with chaotic systems are gradually proposed [17]–[20]. Liu *et al.* [21] proposed combining CS with Arnold scrambling. Zhou *et al.* [22] proposed the encryption and compression scheme in which Logistic map is used to perform key control of measurement matrix. Huang *et al.* [23] proposed an image encryption method in which image was compressed and sampled before scrambling. In contrast, Zhang *et al.* [24] proposed an image encryption scheme in which the frequency domain coefficients of the image are first scrambled and then CS sampling is performed. Zhu and Zhu [25] proposed an image compression-encryption scheme based on CS and chaos. The measurement matrix is generated by Chebyshev map and encryption is performed based on hyperchaotic system. Chai *et al.* [19] proposed an image encryption algorithm in which the measurement matrix is produced by the memristive chaotic system and scramble is performed based on elementary cellular automata. In most of these schemes, the original image is first sampled by CS, and then the measured values obtained from the sampling are scrambled and diffused again by the chaotic map to form the final cipher image. The parameters and initial values of the chaotic system are considered as keys. These encryption schemes are secure against chosen-plaintext attack, but they add too much computational overhead. To relieve the pressure of computation, Huang *et al.* [26] proposed a parallel CS image encryption method. Hu *et al.* [27] proposed a novel image coding scheme in which both the CS sampling and the CS reconstruction are performed in parallel.

Another way is to combine the optical encryption technology with the CS method [28]–[30], such as the double random phase encoding (DRPE) technology is combined with CS to retain the construction robustness of the CS framework itself. Optical encryption scheme DRPE was proposed by Refregier and Javidi [31]. It made use of Fourier transform (FT). Unnikrishnan and Singh [32] introduced the fractional Fourier transform(FRT) theory on the basis of [31], which expanded key space. In order to enhance the security, the random shifting was first introduced in fractional Fourier domains by Hennelly and Sheridan [33]. Based on the good properties of the FRT, sparse representation of two- and three-dimensional images with FRT [34] and a number of encryption methods with FRT were proposed. And Hennelly and Sheridan [35] presented a brief review of the encryption methods with FRT.

With the development of one-dimensional CS methods and theories, the two-dimensional CS method has become a new research hotspot. Zhou N R *et al.* combined two-dimensional CS with the fractional Merlin transform [36] and cyclic shift controlled by hyperchaotic system [37], respectively. Deng *et al.* [38] used a fractional-order random transform to encrypt the sampling values obtained from two-dimensional CS. Yang *et al.* [39] proposed an image compression encryption-scheme based on fractional order hyperchaotic systems combined with two-dimensional CS and DNA encoding. The construction parameters of the CS measurement matrix are controlled by fractional order hyperchaotic systems.

In this paper, a joint image compression and encryption scheme based on CS and FRT is proposed. In this scheme, compression and encryption are combined. Chaotic systems and FRT are added to the CS to improve security. Moreover, plaintext-based key is used to enhance security. The Arnold transformation is used to perform scrambling encryption to hide the energy distribution information of the original image. Chen hyperchaotic system is combined with double random phase encryption based on two-dimensional fractional Fourier transform (2D-FRT). In double random phase encryption, Chen hyperchaotic system is used to produce random phase mask matrices. Double random phase encryption based on 2D-FRT improves security on CS while maintaining reconstruction robustness. The experimental results presented in this paper show the effectiveness of the proposed joint image compression and encryption scheme.

The rest of this paper is organized as follows. A review of CS and FRT is given in Section II. In Section III, the proposed joint image compression and encryption scheme is described. The experimental results and analysis of our new scheme are given in Section IV. Finally, the study's conclusions are presented in Section V.

II. RESEARCH ON COMPRESSIVE SENSING AND 2D-FRT

A. COMPRESSIVE SENSING

CS can obtain the discrete samples of the signal under the condition that the sampling rate is far less than Nyquist frequency, and the signal is sampled and compressed at the same time. For sparse one-dimensional signal $x \in R^N$ and measurement matrix $\Phi \in R^{M+N}(M \ll N)$, the linear measurement value $y \in R^M$ is as follows

$$y = \Phi x \tag{1}$$

Because the dimension of vector y is much smaller than that of vector x, this sampling method has a significant compression effect. Moreover, it has low computational complexity. When the original signal x is reconstructed from the measurement value y and the measurement matrix Φ, in order to find the only original signal from infinite solutions, the

measurement matrix Φ should meet the restricted isometry property (RIP).

Definition 1: For any positive integer $K = 1,2,3,\ldots$, δ_k is the isometry constraint constant of matrix Φ, and it is the minimum value satisfying the Eq.(2)

$$(1-\delta_k)\|x\|_2^2 \le \|\Phi x\|_2^2 \le (1+\delta_k)\|x\|_2^2 \tag{2}$$

where x is any K-sparse vector, Eq.(2) is called RIP. If K is less than and not close to 1, then matrix is said to satisfy RIP.

The row dimension M of the measurement matrix Φ, namely number of measurements, must meet

$$M \ge cK\log(N/K) \tag{3}$$

where c is a constant, K is signal sparsity, and N is column dimension.

According to Eq.(1), for $N \times 1$ non sparse signal f, the $M \times 1$measurement value y is as follows

$$y = \Phi f = \Phi\Psi x = Ax \tag{4}$$

where $A = \Phi\Psi$ is the $M \times N$ matrix called perceptual matrix; Φ is the measurement matrix which meets the RIP; Ψ is $N \times N$ sparse basis; x is $N \times 1$ sparse representation of signal f.

B. FRACTIONAL FOURIER TRANSFORM

The Fourier transform of one-dimensional signal $f(x)$ is defined as

$$F^P\{f(x)\}(u) = \int_{-\infty}^{+\infty} K_p(x,u)f(x)dx \tag{5}$$

where $K_p(x,u)$ is the transform kernel, defined as

$$K_p(x,u) = \begin{cases} A\exp[i\pi(x^2\cot a \\ \quad -2xu\csc a + u^2\cot a)] & a \ne n\pi \\ \delta(x-u) & a = 2n\pi \\ \delta(x+u) & a = (2n+1)\pi \end{cases} \tag{6}$$

where $A = \frac{\exp[-i(\pi\,\mathrm{sgn}(\sin a)/4 - a/2)]}{\sqrt{|\sin a|}}$ is the amplitude, sgn is the signum function, and $a = p\pi/2$ is the angle.

Fractional Fourier transform (FRT) is an extension of the order of traditional Fourier transform (FT), and is widely used in image encryption fields. By degree of transition between fractional order representation function and Fourier transform, we can describe the characteristics of space-time domain and frequency domain at the same time. There are some important properties about FRT:

1) Additivity of order. For different fractional orders p_1 and p_2, which satisfy $F^{p_1}F^{p_2} = F^{p_1+p_2}$. This property is also called rotational additivity.
2) Linearity. Satisfy $F^p[\sum c_n f_n(u)] = \sum c_n[F^p f_n(u)]$, namely linear transformation.
3) Periodicity. Satisfy $F^{p+4} = F^p$, the transformation period is 4. The corresponding rotation angle is $[0,2\pi]$.
4) Invertibility. Satisfy $(F^p)^{-1} = F^{-p}$, F^p and F^{-p} are reversed for each other.

Because the image is two-dimensional data, 2D-FRT is used in this paper. The kernel function of 2D-FRT is as follows:

$$\begin{aligned} K_{p_1,p_2}(x,y,u,v) = {} & \frac{\sqrt{1-j\cot a}\sqrt{1-j\cot\beta}}{2\pi} \\ & \times \exp[(\frac{x^2+u^2}{2\tan a} - \frac{xu}{\sin a})j] \\ & \times \exp[(\frac{x^2+v^2}{2\tan\beta} - \frac{yv}{\sin\beta})j] \end{aligned} \tag{7}$$

where a and β represent the rotation of 2D- FrFT, $a = (p_1\pi)/2$, $\beta = (p_2\pi)/2$. The corresponding two-dimensional transformation forms are:

$$F^{p_1,p_2}(u,v) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K_{p_1,p_2}(x,y,u,v)f(x,y)dxdy \tag{8}$$

Its inverse is

$$f(x,y) = \int_{-\infty}^{\infty}\int_{-\infty}^{\infty} K_{-p_1,-p_2}(x,y,u,v)F^{p_1,p_2}(u,v)dudv \tag{9}$$

FRT is the rotation of time-frequency plane by fractional order which can be regarded as secret key. Because of the linear transformation, the robustness of CS can be preserved.

III. DESIGN OF IMAGE COMPRESSION AND ENCRYPTION ALGORITHM

A. IMAGE COMPRESSION AND ENCRYPTION ALGORITHM

The image compression and encryption scheme proposed in this paper mainly focuses on the improved security of encryption and reconstruction robustness. Therefore, the Arnold transform scrambling and 2D-FRT are added during the process of CS. Four parameters of two two-dimensional FRT are provided by Chen hyperchaotic system. The overall process is shown in Fig. 1. First, the original image is divided into blocks, and the block-by-block parallel compression and encryption operations are obtained. The 256-bit hash value of the image with SHA-256 is used as the initial value of the chaotic system, namely, key. The sampling rate that needs to be allocated for the block is calculated. Then, according to the initial value of the previous step, the chaotic measurement matrix is constructed, and the CS operation is further performed to obtain the initial compressed and encrypted data of the image. At this step, the amount of data will be significantly reduced, facilitating subsequent encryption operations. The block is first scrambled, then the 2D-FRT is used for encryption, and decryption is the reverse of encryption. Here are the specific steps for image compression and encryption scheme:

Step 1: The original image is divided into blocks. Due to the huge amount of image data, images need to be divided into blocks and then processed in parallel for ease of processing and storage. In this paper, the image is evenly divided into blocks of equal width and height. If the number of pixels is insufficient, zero is added. Here let f be the block.

Step 2: Set the proportional parameter of the sampling rate according to the required compression quality. The corresponding relationship is $M = \lceil k^* H^* \sqrt{Img\_size} \rceil$, where M

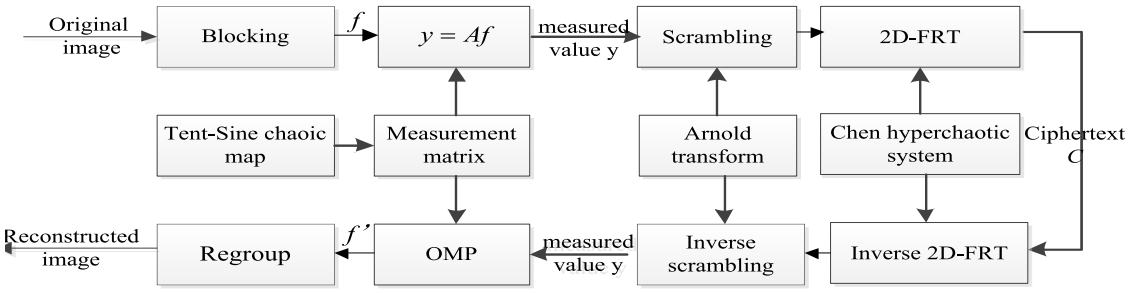


FIGURE 1. Image compression and encryption algorithm based on CS and FRT.

is the number of measurement, M/N is the sampling rate, N is column dimension of measurement matrix, $k > 0$ is the constant coefficient set according to the needs of the compression effect, H is the entropy of the block, and *Img_size* is the total number of pixels of the block. Here k is the proportional parameter to be set. The smaller k is, the greater the compression ratio is.

Step 3: Use SHA256 to obtain the 256-bit hash value of the image. Considering that the entire encryption process shares 8 initial values as the key, each 32 bits of hash value is divided into a group to obtain initial values (r, z_0) for Tent-Sine, (a, b) for Arnold transform and (x, y, z, h) for Chen hyperchaotic system. The Tent-Sine map, Arnold transform, and Chen hyperchaotic system are shown in Eqs.(10),(11) and (12), respectively.

$$x_{n+1} = \begin{cases} (rx_n/2 + (4-r)\sin(\pi x_n)/4) \bmod 1, \\ \qquad x_n < 0.5 \\ (r(1-x_n)/2 + (4-r)\sin(\pi x_n)/4) \bmod 1, \\ \qquad x_n \geq 0.5 \end{cases} \tag{10}$$

where $r \in (0,4)$, $x_n \in [0,1]$.

$$\begin{bmatrix} x_{n+1} \\ y_{n+1} \end{bmatrix} = \begin{bmatrix} 1 & b \\ a & ab+1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} \bmod N \tag{11}$$

where a, b and N are positive integers.

$$\begin{cases} \dot{x} = a(y-x) \\ \dot{y} = dx - xz + cy - h \\ \dot{z} = xy - bz \\ \dot{h} = x + k \end{cases} \tag{12}$$

where $a = 36$, $b = 3$, $c = 28$, $d = -16$, $-0.7 < k < 0.7$.

Step 4: First quantize r and z_0 to (0, 4) and [0, 1], and then construct the chaotic measurement matrix A from the initial value (r, z_0) according to the Algorithm1.

Algorithm1. Measurement matrix constructing based on chaotic system

Input: control parameter $r \in (0, 4)$ of chaotic system, initial value $z_0 \in (0,1)$ of chaotic system, sampling distance $d = 15$ of chaotic system and initial sampling position n_0.

Output: $M \times N$ measurement matrix.

1): Give control parameter r and initial value z_0, and execute n_0+MNd iterations for Tent-Sine. During the iteration, sample chaotic state values with the distance of d as follows:

$$Z(d, r, z_0) = \{z_{n_0+i\times d}\}_{i=0}^{MN-1} \tag{13}$$

where $Z_{n_0+i\times d}$ is the $(n_0 + i \times d)$th chaotic state value. When the sequence accumulates M values, the next value is multiplied by a constant λ and then iterated. The value n_0 is set to avoid the non-chaotic state in the initial iteration of chaotic system.

2): Obtain chaotic sequence $\{w_i\}_{i=0}^{MN-1} = \{1 - 2z_{n_0+i\times d}\}_{i=0}^{MN-1}$ according to chaotic sequence $Z_{n_0+i\times d}$, so change the value of chaotic sequence from (0, 1) to (−1,1).

3): Construct measurement matrix in a column by column way using chaotic sequence $\{w_i\}_{i=0}^{MN-1}$. The measurement matrix is as follows:

$$\Phi = \sqrt{\frac{2}{M}} \begin{pmatrix} w_0 & w_M & \cdots & w_{MN-M} \\ w_1 & w_{M+1} & \cdots & w_{MN-M+1} \\ \vdots & \vdots & \ddots & \vdots \\ w_{M-1} & w_{2M-1} & \cdots & w_{MN-1} \end{pmatrix} \tag{14}$$

where factor $\sqrt{\frac{2}{M}}$ is used to balance the energy before and after sampling.

Step 5: Execute $y = Af$ to obtain the preliminary ciphertext y of the image after encryption and compression processing.

Step 6: First quantize the initial value (a, b) of step 3 as a positive integer, then scramble the relative position of the block by the Arnold transform. Since the first value of the upper left corner after being processed by the Arnold transform does not change, the transform coefficient can be inferred from it. So the value in position (a mod (N), b mod (N)) and the first value of the upper left corner are exchanged. After that, ciphertext z is obtained.

Step 7: Four chaotic sequences are produced by Chen hyperchaotic system with initial value (x, y, z, h) obtained by step 3. Considering that the chaotic sequences are used as the initial value of two 2D-FRT and the FRT period is [0, 4), the value of chaotic sequence is adjusted to [0, 4) by quantized method:

$$k^* = (k \times 10^{14}) \bmod 4 \tag{15}$$

where k is chaotic value, k^* is chaotic value after quantization.

Step 8: The 2D-FRT has two orders as variable parameters and requires the chaotic sequence to provide initial values. Because double random phase encryption is adopted, two 2D-FRTs are performed, and two random matrices are used as a double random phase mask. The two random matrices are given by a hyperchaotic system. The scrambled image ciphertext z is transformed as a whole. The specific double random phase encryption based on 2D-FRT method is as follows:

1)The ciphertext obtained in the previous step is divided into left and right two parts z_r and z_i. Then take the corresponding value as the real part and the imaginary part of the complex number to get the expression

$$T(x, y) = z_r(x, y) + z_i(x, y) \tag{16}$$

where $T(x, y)$ is a new complex image.

2)The two random phase mask matrices R_1 and R_2 are generated by the Chen hyperchaotic system and the two orders 2D-FRT is performed on $T(x, y)$

$$C(x, y) = F^{p_2}\{F^{p_1}\{T(x, y)\exp[iR_1(x, y)]\}\exp[iR_2(x, y)]\} \tag{17}$$

Follow the above steps to get the final ciphertext.

B. IMAGE DECOMPRESSION AND DECRYPTION ALGORITHM

The decompression and decryption scheme are the inverse of the compression and encryption scheme. Sampling and reconstruction are asymmetric in CS theory. The computational complexity of compression and encryption is low. The computational complexity of reconstruction is higher than that of compression and encryption. And the methods applied in sampling and reconstruction are different. Specific steps of the decompression and decryption are as follows:

Step 1: Iterate the Chen hyperchaotic system by the initial key (a, b, c, d), and get four key streams.

Step 2: Because the 2D-FRT is an invertible transform, namely $(F^p)^{-1} = F^{-p}$. So the image cipher text is initially decrypted, the negative value of the chaotic sequence in Step 1 is used to implement the inverse transform,

$$T(x, y) = F^{-p_1}\{F^{-p_2}\{C(x, y)\exp[-iR_2(x, y)]\} \times \exp[-iR_1(x, y)]\} \tag{18}$$

Step 3: Decompose the complex image $T(x, y)$ into a real image,

$$\begin{cases} z_r(x, y) = real\ [T(x, y)] \\ z_i(x, y) = imag\ [T(x, y)] \end{cases} \tag{19}$$

Then follow the real part to the left and the imaginary part to the right to restore the ciphertext z.

Step 4: The Arnold transform determined by the key (a, b) restores the position (a mod (N), b mod (N)) of the image block. First, the position of the first value of the ciphertext is exchanged with the first position of the ciphertext. Then the image block is iteratively restored according to the Arnold transformation to get the ciphertext y.

Step 5: The Tent-Sine chaotic map is iterated by the key (r, z_0) to obtain the chaotic measurement matrix used in the encryption. The OMP reconstruction algorithm is applied to the ciphertext obtained in the previous step, and the redundant DCT dictionary is used in combination to recover the blocks. The original image is obtained by recombining the block image.

IV. EXPERIMENTAL RESULTS AND ANALYSIS

For the new compression and encryption scheme, we conducted security test, compression performance test and robustness test. The compression and encryption are implemented in MATLAB R2012a running on a personal computer with a 3.4-GHz processor and 4GB memory.

A. EXPERIMENTAL RESULTS

Test images are obtained from images taken by the Hubble Space Telescope in public and USC-SIPI image database. Given that the difference in pixel distribution of different images will affect the compression ratio and encryption effect of algorithm, we use three grayscale images commonly used in image processing technology to test security, robustness and compression performance of the compression and encryption algorithm proposed in this paper. The images are M104, ARP273, and NGC6302 with 256 × 256. In the experiment, in order to display the visual effect of the ciphertext, the amplitude and phase values of the ciphertext are put together. The test results are shown in Fig.2, in which (a), (d) and (g) are original images, (b), (e), and (h) are ciphertexts processed by encryption and compression. The size of ciphertext is 181 × 181. It can be seen that the ciphertext does not reveal the plaintext information. Fig. 2 (c), (f) and (i) are the reconstructed images. It can be seen that the reconstructed image can retain the plaintext content well.

B. COMPRESSION PERFORMANCE

Compression performance is measured by compression ratio and PSNR. PSNR is used to measure image compression quality.

$$PSNR = 10 \times \log_{10}\left(\frac{x_{peak}^2}{MSE}\right) \tag{20}$$

where x_{peak} represents signal peak value, and MSE represents mean square error.

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}(\hat{f}(i, j) - f(i, j))^2 \tag{21}$$

where $\hat{f}(i, j)$ and $f(i, j)$ represent original image and testing image, respectively. M and N represent the height of the image and the width of the image, respectively.

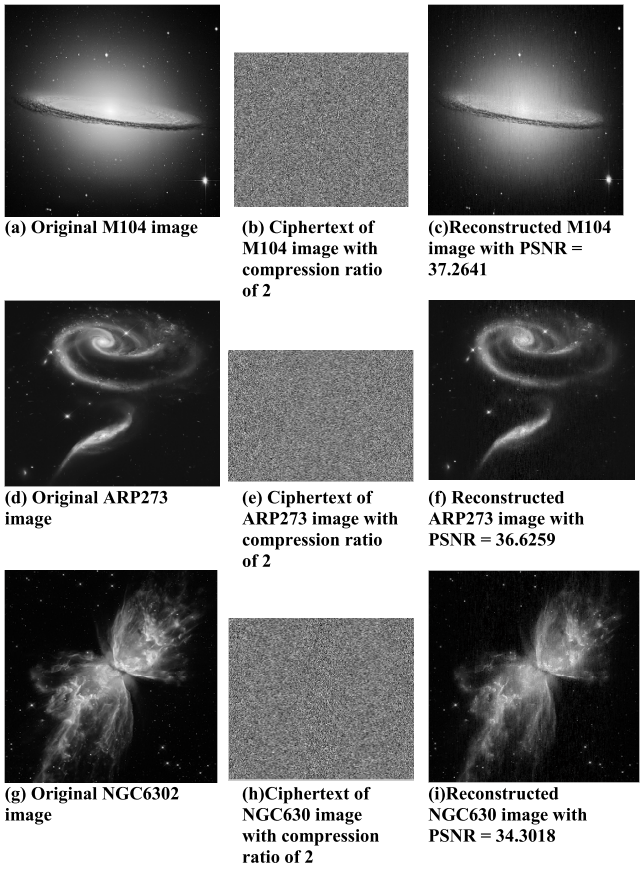


FIGURE 2. Original image, ciphertext and reconstructed image. (a) Original M104 image. (b) Ciphertext of M104 image with compression ratio of 2. (c) Reconstructed M104 image with PSNR=37.2641. (d) Original ARP273 image. (e) Ciphertext of ARP273 image with compression ratio of 2. (f) Reconstructed ARP273 image with PSNR=36.6259. (g) Original NGC6302 image. (h) Ciphertext of NGC6302 image with compression ratio of 2. (i) Reconstructed NGC6302 image with PSNR=34.3081.

TABLE 1. Lena image quality comparison at different compression ratios.

PSNR / CR	Ref.38	Our scheme
7.1111	12.30	27.6305
4.000	17.42	28.6346
2.500	22.01	31.4316
1.7778	26.04	36.7904

For a $M \times N$ image, the compression ratio CR is calculated as follows:

$$CR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} r_b(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N} r_c(i,j)} = \frac{\bar{r}_b}{\bar{r}_c} \tag{22}$$

where $\bar{r}_b$ represents average value of image pixel code length r_b, $\bar{r}_c$ represents average value of image pixel code length r_c.

Since image Lena is employed by most of existing methods, we select image Lena to perform the compare operation. The test results are shown in Table 1.

Reference [38] is an image compression-encryption scheme combining 2D CS with discrete fractional random transform. From Table 1, we can see that the reconstructed image using the compression and encryption method in this paper has better image quality. That is to say with the same reconstructed effect, our scheme can achieve a larger compression ratio.

TABLE 2. Avalanche effect test results for changing the plaintext and keys.

CR	Plaintext	Key z_0	Key a	Key b	Key x	Key y	Key z	Key h
1.32	0.4604	0.4611	0.4566	0.4533	0.4582	0.4734	0.4722	0.4792
1.94	0.4612	0.4662	0.4605	0.4551	0.4603	0.4783	0.4756	0.4810
4.00	0.4643	0.4606	0.4639	0.4560	0.4612	0.4771	0.4729	0.4814
8.46	0.4688	0.4688	0.4630	0.4557	0.4622	0.4788	0.4737	0.4823

C. KEY SPACE ANALYSIS

The key space of the image encryption system needs to be at least 2^{128} to be effective against exhaustive attacks. In this encryption scheme, the key is the initial value (r, z_0) of the Tent-Sine chaotic map, the initial value (a, b) of Arnold transform, and the initial value (x, y, z, h) of the Chen hyperchaotic system that correspond to the construction of chaotic measurement matrix, scrambling encryption and the construction of the double random phase mask matrix. Because the key is related to the plaintext, and the plaintext hash value with SHA256 is divided to get the key, the key space is $K = 2^{256}$. It can be seen that this encryption scheme has a large enough key space to withstand exhaustive attacks.

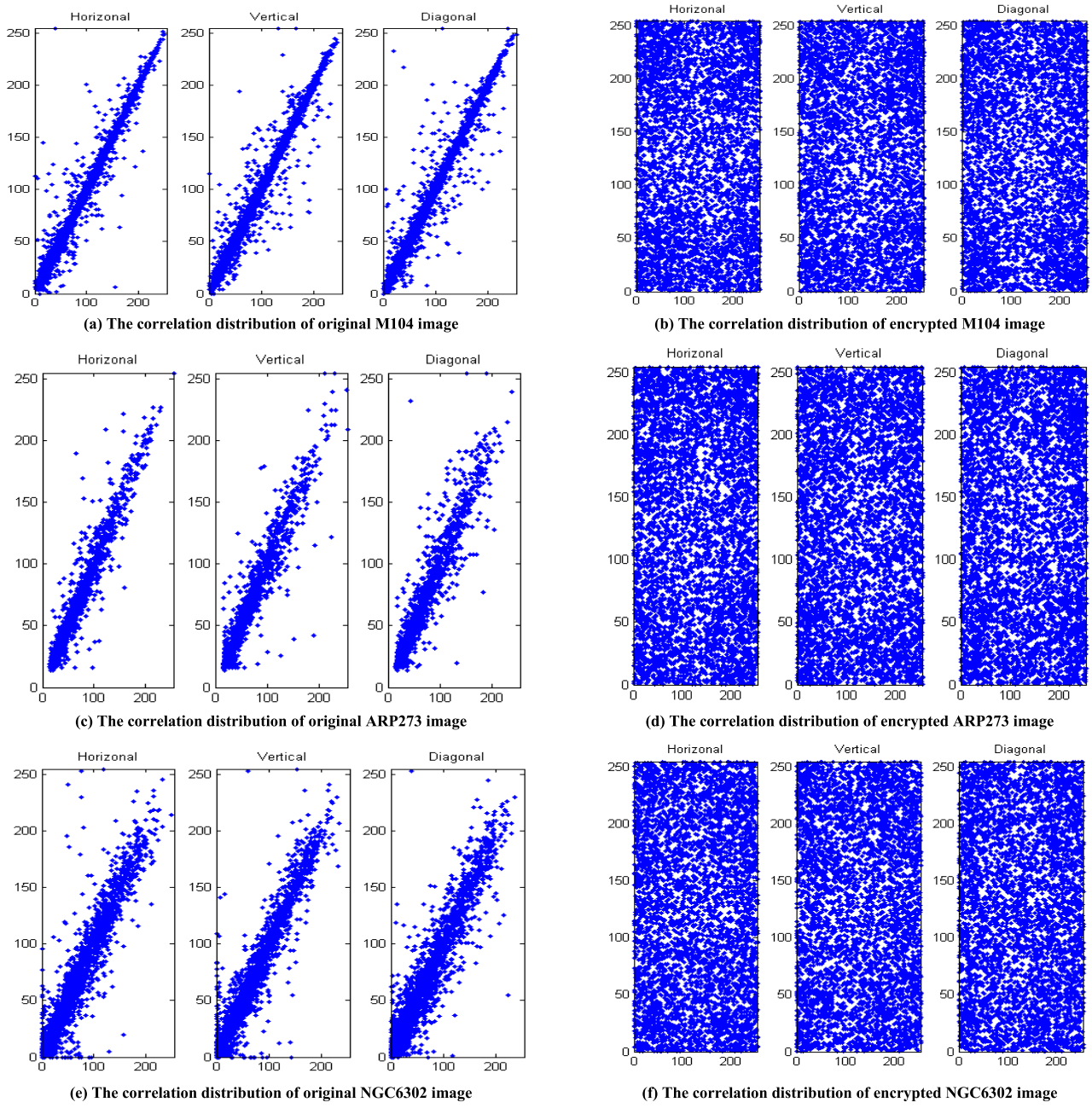
D. AVALANCHE EFFECT TEST

Avalanche effect refers to the effect that when the input of encryption algorithm changes slightly, ciphertext changes greatly. This property ensures better randomization characteristics, making it difficult for attackers to obtain input from the output. In the following tests, the key (r, z_0) of the measurement matrix, the scrambled key (a, b), and the 2D-FRT key (x, y, z, h) are artificially changed by one bit, and then the change of the ciphertext is compared. The ideal rate of change is 50%. Table 2 shows the avalanche effect test results with a change of one bit for the plaintext and the key respectively.

From Table 2, we can see that the encryption algorithm can guarantee to approach the ideal value of avalanche effect. The avalanche effect of the algorithm benefits from two aspects. On the one hand, initial value sensitivity of the chaotic map provides good randomness; on the other hand, random phase mask matrices used in FRT encryption can well spread the small changes of the key.

E. CORRELATION TEST

The correlation of adjacent pixels in an image is a criterion for evaluating the scrambling degree of an encryption algorithm. Only by destroying the pixel correlation of the original image, the attacker cannot infer the adjacent pixel value. Thereby the security of the image information is ensured. In the test, 5000 pixels are randomly selected in the horizontal, vertical, and diagonal directions. The correlation distribution of pixels before and after encryption is shown in Fig. 3.



(a) The correlation distribution of original M104 image

(b) The correlation distribution of encrypted M104 image

(c) The correlation distribution of original ARP273 image

(d) The correlation distribution of encrypted ARP273 image

(e) The correlation distribution of original NGC6302 image

(f) The correlation distribution of encrypted NGC6302 image

FIGURE 3. The pixel correlation distributions of original and encrypted image. (a) The correlation distribution of original M104 image. (b) The correlation distribution of encrypted M104 image. (c) The correlation distribution of original ARP273 image. (d) The correlation distribution of encrypted ARP273 image. (e) The correlation distribution of original NGC6302 image. (f) The correlation distribution of encrypted NGC6302 image.

According to the test results, the distributions of the three images before encryption in the three horizontal, vertical, and diagonal directions show a certain rule. Since this rule is related to the plaintext image information. So if you cannot change the distribution of this rule, it will be insecure. After encryption is performed by the encryption algorithm proposed, the distribution of pixels is uniform. The algorithm destroys the correlation between adjacent pixels of the image, achieves a good scrambling effect, and ensures image information security. The following quantitative analysis shows that the encryption algorithm achieves the purpose of destroying the correlation of adjacent pixels in the image.

The calculation of correlation is as follows

$$C_r = \frac{N\sum_{j=1}^{N}(x_j y_j) - (\sum_{j=1}^{N} x_j)(\sum_{j=1}^{N} y_j)}{\sqrt{(N\sum_{j=1}^{N} x_j^2 - (\sum_{j=1}^{N} x_j)^2)}\sqrt{(N\sum_{j=1}^{N} y_j^2 - (\sum_{j=1}^{N} y_j)^2)}} \quad (23)$$

where x_i and y_j represent adjacent pixel values, N represents number of pixels. The test results are shown in Table 3.

From Table 3, it can be seen that before encryption, correlation coefficients in three directions of three images are all close to 1, that is, they have strong correlation.

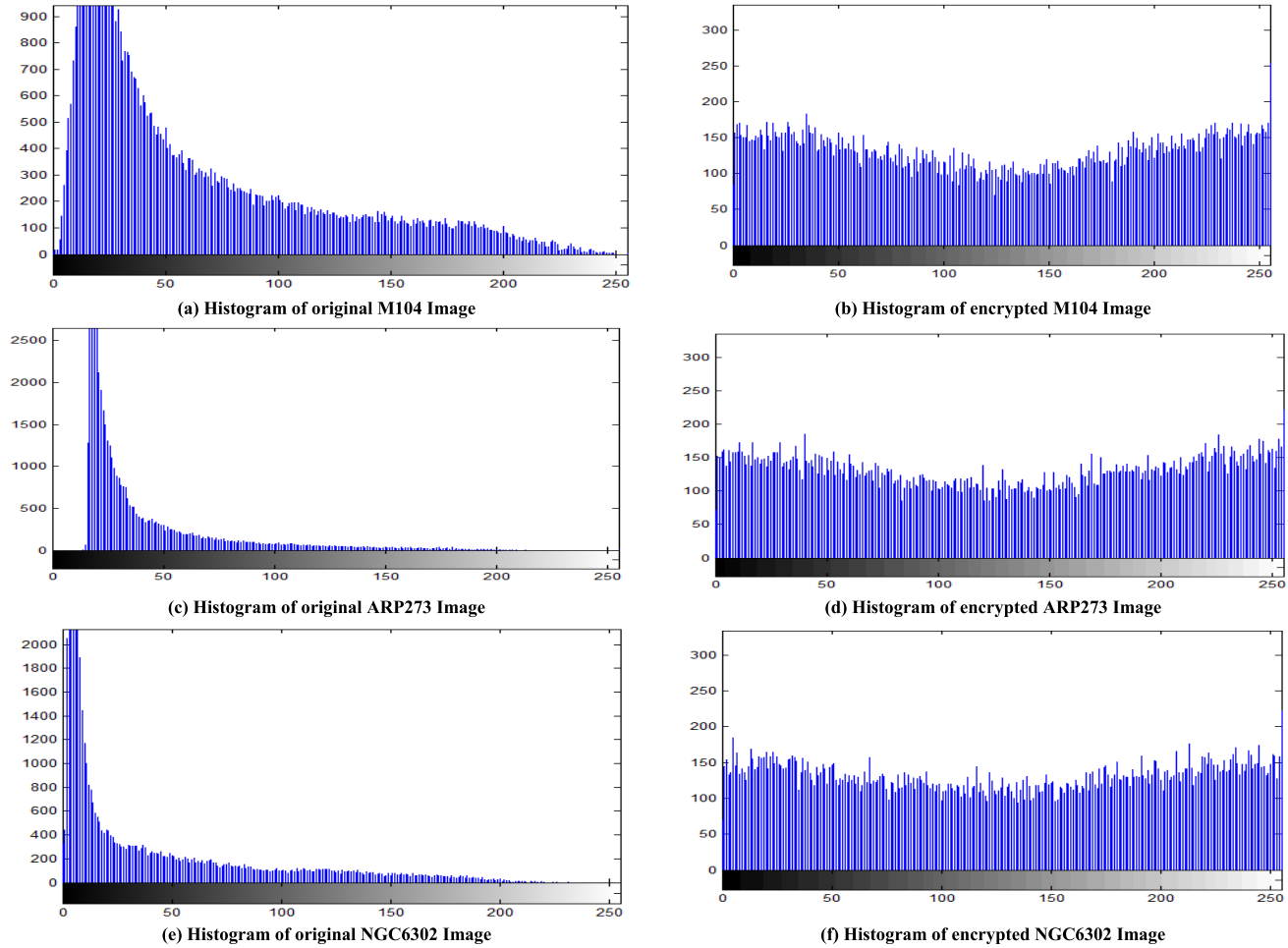


FIGURE 4. Histogram of original and encrypted image. (a) Histogram of original M104 image. (b) Histogram of encrypted M104 image. (c) Histogram of original ARP273 image. (d) Histogram of encrypted ARP273 image. (e) Histogram of original NGC6302 image. (f) Histogram of encrypted NGC6302 image.

TABLE 3. Correlation coefficient of adjacent pixels.

Test images	Horizontal	Vertical	Diagonal
Original M104 image	0.9409	0.9735	0.9176
Encrypted M104 Image	0.0021	0.0151	0.0091
Original ARP273 Image	0.9549	0.9474	0.9080
Encrypted ARP273 Image	0.0120	0.0140	0.0130

TABLE 4. Information entropy test results.

Test images	Plaintext information entropy	Ciphertext information entropy	Ideal value
M104	7.3158	7.9861	8.0000
ARP273	5.3286	7.8964	8.0000
NGC6302	5.9905	7.9245	8.0000

After encryption, the correlation coefficient in the horizontal, vertical, and diagonal directions are all reduced, and is close to zero. Therefore, the test results verify that the compression encryption algorithm satisfies the security requirements.

F. HISTORGRAM ANALYSIS

In the field of image encryption, the distribution of pixels in the histogram before and after encryption is often used to judge the quality of the encryption algorithm. The test result is shown in Fig. 4.

Fig.4(a), Fig.4(c) and Fig.4(e) are the original images. The histogram distribution presents a certain rule. The attacker will probably infer the original image information through this rule. So a good encryption algorithm must be able to hide this rule. As shown in Fig.4(b), Fig.4(d), and Fig.4(f), the histograms of the encrypted images show a nearly uniform distribution of pixels. It makes it difficult for attackers to get useful statistics from the ciphertext image.

G. INFORMATION ENTROPY TEST

The information entropy characterizes the degree of confusion in the ciphertext. Table 4 lists the entropy values of the three images before and after encryption.

From Table 4, it can be seen that the image data exhibits good randomness after being processed by the compression and encryption algorithm proposed.

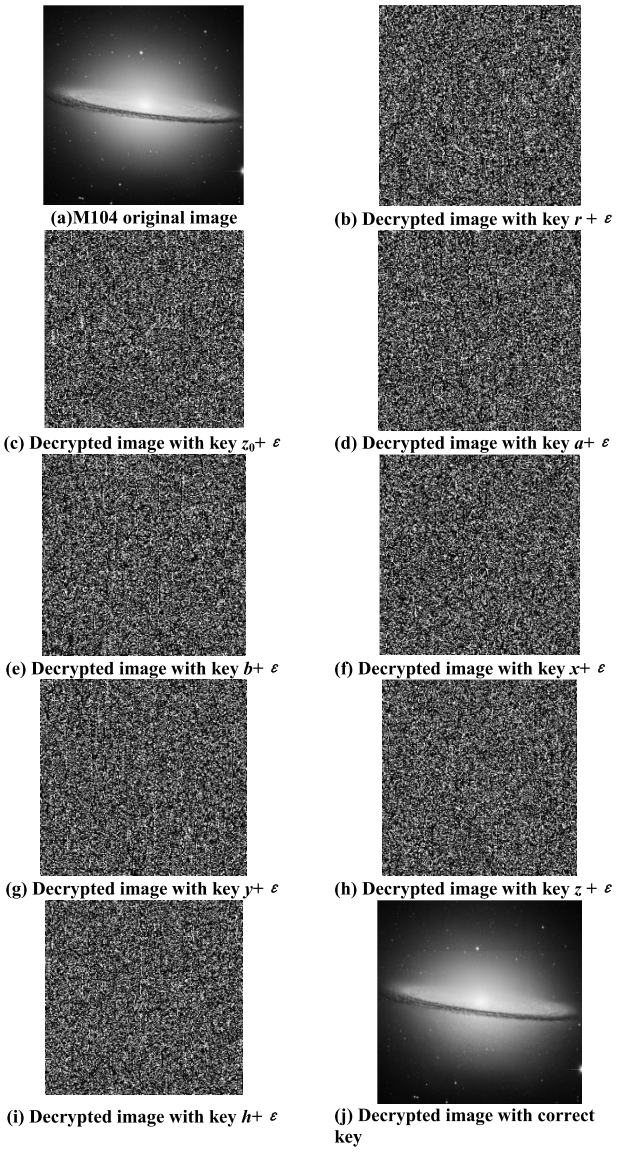


FIGURE 5. Decryption image with small changed keys and correct key. (a) M104 original image. (b) Decrypted image with key $r+\varepsilon$. (c) Decrypted image with key $z_0+\varepsilon$. (d) Decrypted image with key $a+\varepsilon$. (e) Decrypted image with key $b+\varepsilon$. (f) Decrypted image with key $x+\varepsilon$. (g) Decrypted image with key $y+\varepsilon$. (h) Decrypted image with key $z+\varepsilon$. (i) Decrypted image with key $h+\varepsilon$. (j) Decrypted image with correct key.

H. KEY SENEITIVITY TEST

The key sensitivity refers to that the key will lose its effect for decryption when a small change to key value occurs. The algorithm proposed uses 8 values as the key. In order to complete the test, a small change $\varepsilon = (2\times \text{rand}()-1)\times 10^{-10}$ is performed for each key, where rand() is used to generate a random number from 0 to 1. When the changed key is used for decryption, the result is shown in Fig. 5.

It can be seen from Fig.5(b) to Fig.5(i), we cannot decrypt the plaintext for any key change. The security attribute of the key sensitivity in encryption algorithm proposed benefits from the chaotic map. The chaotic measurement matrix is constructed by Tent-Sine map. Unlike other image encryption schemes based on FRT [32], [33], the double random phase mask matrix is also constructed by the chaotic map, that is Chen hyperchaotic system. So the small changes in the key will cause the construction of the matrices to be very different. Therefore, the security of the algorithm is fully guaranteed.

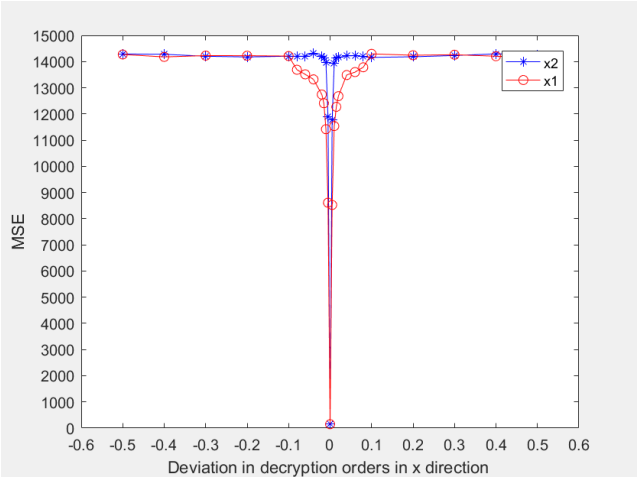


FIGURE 6. Graph of deviation in decryption orders in the x direction from the correct values against the resultant MSE.

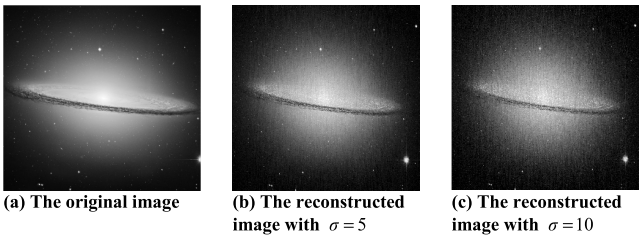


FIGURE 7. Reconstructed image disturbed by noise. (a) The original image. (b) The reconstructed image with $\sigma = 5$. (c) The reconstructed image with $\sigma = 10$.

At the same time, we examine sensitivities of the fractional orders. For comparison, we encrypt image Lena. The ciphertext image obtained from image Lena is decrypted with the correct order and the modified order, and then the difference between the original image and the decrypted image is measured using MSE in Eq.(21). Fig.6 shows the mean square error curves of fractional orders in x direction under different deviation degrees.

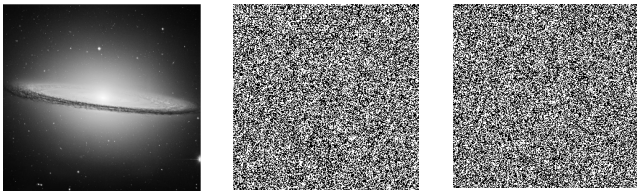
From Fig.6, we can see that the sensitivity of the fractional orders appears better than the equivalent fractional orders in analogous methods [32], [33].

I. RECONSTRUCTION ROBUSTNESS TEST

In communication environment, ciphertext image is often easily disturbed and destroyed by noise, such as the deep-space transmission environment is characterized by its high bit error rate, so reconstruction robustness is a valuable feature of compression and encryption algorithm. Therefore, when transmitting ciphertext, it must be able to guarantee the robustness of ciphertext. That is, when the ciphertext is changed due to interference, it can still recover some useful information. For this test, Gaussian noise is added to each

TABLE 5. Comparison with AES.

Scheme	Correlation coefficient of adjacent pixels		
	Horizontal	Vertical	Diagonal
Our scheme	**0.0021~0.0120**	0.0140~0.0151	**0.0091~0.0130**
AES	0.0042~0.0125	0.0102~0.0126	0.0277~0.0313



(a) The original image (b) The reconstructed image with $\sigma = 5$ (c) The reconstructed image with $\sigma = 10$

FIGURE 8. Reconstructed image using AES under Gaussian noise. (a) The original image. (b) The reconstructed image with $\sigma = 5$. (c) The reconstructed image with $\sigma = 10$.

element of the ciphertext amplitude and phase:

$$C' = C + \sigma G \tag{24}$$

where G represents Gaussian noise and σ represents intensity factor. C and C' represent ciphertext and ciphertext disturbed by noise respectively. Fig.7 gives the results of reconstructed effect disturbed by noise.

Fig. 7(a) is the original image and Fig. 7(b) is the reconstructed image with $\sigma = 5$. The PSNR value of the image can reach 30.9765. Fig. 7(c) is the reconstructed image with $\sigma = 10$. Although the image quality suffers a great loss, it can still distinguish the original image information and its PSNR value is 28.2765. It can be seen that with the increase of noise intensity, the quality of reconstructed image decreases. However, it can also be seen that even if the noise intensity reaches 10, the main content of the corresponding reconstructed image is still very clear. The experimental result shows that the compression and encryption algorithm has reconstruction robustness and is suitable for situations in which the transmission environment is susceptible to interference.

J. PERFORMANCE COMPARISON WITH THE TRADITIONAL ENCRYPTION ALGORITHM

In this section, we provide comparisons with Advanced Encryption Standard (AES) encryption algorithm. We encrypted scrambled measured value with 128 bits AES and cipher block chaining (CBC) mode. Table 5 shows the comparison results for the correlation coefficient of adjacent pixels.

From Table 5, it can be seen that our scheme is slightly better than AES in horizontal and diagonal correlation coefficient.

Fig. 8 shows the results of reconstructed effect using AES under Gaussian noise. Fig. 8(a) is the original image and Fig. 8(b) is the reconstructed image with $\sigma = 5$. The PSNR value of the image is 4.5039. Fig. 8(c) is the reconstructed image with $\sigma = 10$ and the PSNR is 4.5573.

Compare Fig.7 with Fig.8, we can see the proposed scheme have better reconstruction robustness than AES.

V. CONCLUSION

In this paper, an image compression and encryption scheme based on CS and Fourier transform was proposed. The scheme not only ensures the security, but also preserves the reconstruction robustness of CS. Firstly, the image is sampled and compressed with chaotic measurement matrix. At the same time, encryption is implemented to obtain preliminary compressed and encrypted image data. Then, since the leakage of the original image energy information is a disadvantage of compressive sensing applied to encryption, the Arnold transformation is applied to implement scrambling encryption to hide the energy distribution information of the original image. Finally, the scrambled image data is divided into two parts, amplitude and phase, so that it is convenient to apply 2D-FRT for double random phase encryption. The advantage of using 2D-FRT encryption is that it can guarantee high security and preserve the reconstruction robustness of CS, and 2D-FRT is easy to implement with optical hardware. The test results show that the proposed compression and encryption scheme has high security, good compression performance and reconstruction robustness.

REFERENCES

[1] A. Orsdemir, "On the security and robustness of encryption via compressed sensing," in *Proc. MILCOM*, San Diego CA, USA, 2008, pp. 1040–1046.

[2] L. Gan, "Block compressed sensing of natural images," in *Proc. 15th Int. Conf. Digit. Signal Process.*, Cardiff, U.K., Jul. 2007, pp. 403–406.

[3] M. Sarkis and K. Diepold, "Depth map compression via compressed sensing," in *Proc. 16th IEEE Int. Conf. Image Process. (ICIP)*, Cairo, Egypt, Nov. 2009, pp. 737–740.

[4] Z.-M. Du, G.-H. Geng, and Y.-Y. He, "A 2-D geometric signal compression method based on compressed sensing," *Acta Automatica Sinica*, vol. 38, no. 11, pp. 1841–1846, Nov. 2012.

[5] J. Yang, W. E. I. Sha, H. Chao, and Z. Jin, "High-quality image restoration from partial mixed adaptive-random measurements," *Multimedia Tools Appl.*, vol. 75, no. 11, pp. 6189–6205, Mar. 2015.

[6] J. Sun, G. Han, Z. Zeng, and Y. Wang, "Memristor-based neural network circuit of full-function pavlov associative memory with time delay and variable learning rate," *IEEE Trans. Cybern.*, to be published, doi: 10.1109/TCYB.2019.2951520.

[7] W. Shi, F. Jiang, S. Liu, and D. Zhao, "Image compressed sensing using convolutional neural network," *IEEE Trans. Image Process.*, vol. 29, pp. 375–388, Jul. 2020.

[8] Q. Wang, M. Wei, X. Chen, and Z. Miao, "Joint encryption and compression of 3D images based on tensor compressive sensing with non-autonomous 3D chaotic system," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 1715–1734, Jan. 2017.

[9] R. Tan, S.-Y. Chiu, H. H. Nguyen, D. K. Y. Yau, and D. Jung, "A joint data compression and encryption approach for wireless energy auditing networks," *ACM Trans. Sensor Netw.*, vol. 13, no. 2, pp. 1–32, Jun. 2017.

[10] Y. Rachlin and D. Baron, "The secrecy of compressed sensing measurements," in *Proc. 46th Annu. Allerton Conf. Commun., Control, Comput.*, Monticello, IL, USA, Sep. 2008, pp. 813–817.

[11] G. S. Zhang, *Application of Compressed Sensing for Secure Image Coding*. Beijing, China: WASA, 2010, pp. 220–224.

[12] X. P. Zhang, "Compressing encrypted image using compressive sensing," in *Proc. 7th Int. Conf. Intell. Inf. Hiding Multimedia Signal*, Oct. 2011, pp. 222–225.

[13] J. Sun, Y. Wu, G. Cui, and Y. Wang, "Finite-time real combination synchronization of three complex-variable chaotic systems with unknown parameters via sliding mode control," *Nonlinear Dyn.*, vol. 88, no. 3, pp. 1677–1690, Feb. 2017.

[14] J. Sun, X. Zhao, J. Fang, and Y. Wang, "Autonomous memristor chaotic systems of infinite chaotic attractors and circuitry realization," *Nonlinear Dyn.*, vol. 94, no. 4, pp. 2879–2887, Aug. 2018.

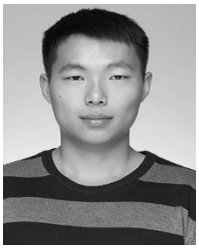
[15] Z. Liu, Q. Guo, L. Xu, M. A. Ahmad, and S. Liu, "Double image encryption by using iterative random binary encoding in gyrator domains," *Opt. Express*, vol. 18, no. 11, pp. 12033–12043, May 2010.
[16] Y. Luo, X. Ouyang, J. Liu, and L. Cao, "An image encryption method based on elliptic curve ElGamal encryption and chaotic systems," *IEEE Access*, vol. 7, pp. 38507–38522, 2019.
[17] D. Xiao, L. Wang, T. Xiang, and Y. Wang, "Multi-focus image fusion and robust encryption algorithm based on compressive sensing," *Opt. Laser Technol.*, vol. 91, pp. 212–225, Jun. 2017.
[18] Z. Gao, C. Xiong, L. Ding, and C. Zhou, "Image representation using block compressive sensing for compression applications," *J. Vis. Commun. Image Represent.*, vol. 24, no. 7, pp. 885–894, Oct. 2013.
[19] X. Chai, X. Zheng, Z. Gan, D. Han, and Y. Chen, "An image encryption algorithm based on chaotic system and compressive sensing," *Signal Process.*, vol. 148, pp. 124–144, Jul. 2018.
[20] X. Chai, Z. Gan, Y. Chen, and Y. Zhang, "A visually secure image encryption scheme based on compressive sensing," *Signal Process.*, vol. 134, pp. 35–51, May 2017.
[21] X. Liu, Y. Cao, P. Lu, X. Lu, and Y. Li, "Optical image encryption technique based on compressed sensing and Arnold transformation," *Optik*, vol. 124, no. 24, pp. 6590–6593, Dec. 2013.
[22] N. Zhou, A. Zhang, F. Zheng, and L. Gong, "Novel image compression-encryption hybrid algorithm based on key-controlled measurement matrix in compressive sensing," *Opt. Laser Technol.*, vol. 62, pp. 152–160, Oct. 2014.
[23] X. Huang, G. Ye, H. Chai, and O. Xie, "Compression and encryption for remote sensing image using chaotic system," *Secur. Commun. Netw.*, vol. 8, no. 18, pp. 3659–3666, Jun. 2015.
[24] Y. Zhang, J. Zhou, F. Chen, L. Y. Zhang, K.-W. Wong, X. He, and D. Xiao, "Embedding cryptographic features in compressive sensing," *Neurocomputing*, vol. 205, pp. 472–480, Sep. 2016.
[25] S. Zhu and C. Zhu, "A new image compression-encryption scheme based on compressive sensing and cyclic shift," *Multimedia Tools Appl.*, vol. 78, no. 15, pp. 20855–20875, Mar. 2019.
[26] R. Huang, K. H. Rhee, and S. Uchida, "A parallel image encryption method based on compressive sensing," *Multimedia Tools Appl.*, vol. 72, no. 1, pp. 71–93, 2014.
[27] G. Hu, D. Xiao, Y. Wang, T. Xiang, and Q. Zhou, "Securing image information using double random phase encoding and parallel compressive sensing with updated sampling processes," *Opt. Lasers Eng.*, vol. 98, pp. 123–133, Nov. 2017.
[28] B. Deepan, C. Quan, Y. Wang, and C. J. Tay, "Multiple-image encryption by space multiplexing based on compressive sensing and the double-random phase-encoding technique," *Appl. Opt.*, vol. 53, no. 20, pp. 4539–4547, Jul. 2014.
[29] P. Lu, Z. Xu, X. Lu, and X. Liu, "Digital image information encryption based on compressive sensing and double random-phase encoding technique," *Optik*, vol. 124, no. 16, pp. 2514–2518, Aug. 2013.
[30] D. Zhang, X. Liao, B. Yang, and Y. Zhang, "A fast and efficient approach to color-image encryption based on compressive sensing and fractional Fourier transform," *Multimedia Tools Appl.*, vol. 77, no. 2, pp. 2191–2208, Jan. 2017.
[31] P. Refregier and B. Javidi, "Optical image encryption based on input plane and Fourier plane random encoding," *Opt. Lett.*, vol. 20, no. 7, pp. 767–769, Apr. 1995.
[32] G. Unnikrishnan, "Double random fractional Fourier-domain encoding for optical security," *Opt. Eng.*, vol. 39, no. 11, pp. 2853–2859, Nov. 2000.
[33] B. Hennelly and J. T. Sheridan, "Optical image encryption by random shifting in fractional Fourier domains," *Opt. Lett.*, vol. 28, no. 4, pp. 269–271, Feb. 2003.
[34] A. Koç, B. Bartan, E. Gundogdu, T. Çukur, and H. M. Ozaktas, "Sparse representation of two- and three-dimensional images with fractional Fourier, hartley, linear canonical, and Haar wavelet transforms," *Expert Syst. Appl.*, vol. 77, pp. 247–255, Jul. 2017.
[35] B. M. Hennelly and J. T. Sheridan, "Image encryption and the fractional Fourier transform," *Optik*, vol. 114, no. 6, pp. 251–265, May 2003.
[36] N. Zhou, H. Li, D. Wang, S. Pan, and Z. Zhou, "Image compression and encryption scheme based on 2D compressive sensing and fractional Mellin transform," *Opt. Commun.*, vol. 343, pp. 10–21, May 2015.
[37] N. Zhou, S. Pan, S. Cheng, and Z. Zhou, "Image compression–encryption scheme based on hyper-chaotic system and 2D compressive sensing," *Opt. Laser Technol.*, vol. 82, pp. 121–133, Aug. 2016.
[38] J. Deng, S. Zhao, Y. Wang, L. Wang, H. Wang, and H. Sha, "Image compression-encryption scheme combining 2D compressive sensing with discrete fractional random transform," *Multimedia Tools Appl.*, vol. 76, no. 7, pp. 10097–10117, 2017.
[39] Y.-G. Yang, B.-W. Guan, J. Li, D. Li, Y.-H. Zhou, and W.-M. Shi, "Image compression-encryption scheme based on fractional order hyper-chaotic systems combined with 2D compressed sensing and DNA encoding," *Opt. Laser Technol.*, vol. 119, Nov. 2019, Art. no. 105661.

MIAO ZHANG received the Ph.D. degree in computer science and technology from the Harbin Institute of Technology, in 2018. She is a Doctor with the Harbin Institute of Technology, Weihai. From 2004 to 2006, she was an Assistant Lecturer with the Harbin Institute of Technology. Since 2006, she has been a Lecturer with the Harbin Institute of Technology. Her current research interests include the areas of chaos cryptography, information security, and image processing.

XIAO-JUN TONG is currently a Professor and a Ph.D. Supervisor with the Harbin Institute of Technology. Her current research interests are in the areas of chaos cryptography and information security. She is a member of Program Committee for the International Workshop on Chaos Fractals Theories and Applications.

JIE LIU received the B.Eng. degree from the Department of Information Security, PLA Information Engineering University, in 2003, and the M.E. degree from the Harbin University of Science and Technology, in 2007. He is currently pursuing the Ph.D. degree with the Department of Computer Science and Technology, Harbin Institute of Technology. His research interests include chaos cryptosystems, coding-based cryptosystems, and key management.

ZHU WANG is currently a Professor with the Harbin Institute of Technology. His current research interests are wireless sensor networks and networking technology, and single processing.



JINLONG LIU is currently pursuing the M.S. degree in computer science and technology with the Harbin Institute of Technology. His research interests include chaos cryptography and image processing.

BAOLONG LIU received the M.S. degree in computer science and technology from the Harbin Institute of Technology, in 2018. His research interests are chaos cryptography and image processing.

JING MA is an Engineer with the Science and Technology on Information Assurance Laboratory. Her interest is information security.